IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

| | |
|---|---|
| SRI INTERNATIONAL, INC., a California Corporation,<br><br>Plaintiff and Counterclaim-Defendant,<br><br>v.<br><br>INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia corporation, and SYMANTEC CORPORATION, a Delaware corporation,<br><br>Defendants and Counterclaim-Plaintiffs. | C. A. No. 04-1199 (SLR)<br><br>**Public Version** |

**DECLARATION OF PHILLIP A. PORRAS IN SUPPORT OF SRI INTERNATIONAL, INC.'S RESPONSES TO DEFENDANTS' JOINT MOTION FOR SUMMARY JUDGMENT THAT SRI INTERNATIONAL, INC.'S PATENTS ARE INVALID FOR FAILURE TO DISCLOSE BEST MODE AND DEFENDANTS' JOINT MOTION FOR SUMMARY JUDGMENT OF INVALIDITY PURSUANT TO 35 U.S.C. §§ 102 & 103**

Dated: June 30, 2006

FISH & RICHARDSON P.C.

John F. Horvath (#4557)
FISH & RICHARDSON P.C.
919 N. Market St., Ste. 1100
P.O. Box 1114
Wilmington, DE 19889-1114
Telephone: (302) 652-5070
Facsimile: (302) 652-0607

Howard G. Pollack (CA Bar No. 162897)
Katherine D. Prescott (CA Bar No. 215496)
FISH & RICHARDSON P.C.
500 Arguello St., Ste. 500
Redwood City, CA 94063
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

Attorneys for Plaintiff and Counterclaim Defendant
SRI INTERNATIONAL, INC.

I, Phillip A. Porras, declare as follows:

**GENERAL**

1. I am currently employed by SRI International, Inc. in the Computer Science Laboratory as Program Director. My work address is 333 Ravenswood Avenue, Menlo Park, California, 94025, USA. I have personal knowledge of the matters stated in this declaration.

2. I am one of the named inventors of the patents-in-suit, U.S. Patent Nos. 6,321,338, 6,484,203, 6,711,615, and 6,708,212.

**EMERALD 1997**

3. I began working at SRI in September, 1996.

4. While at SRI, I have worked on the Event Monitoring Enabling Responses to Anomalous Live Disturbances (EMERALD) projects.

5. Shortly after I joined SRI, Peter Neumann and I drafted a paper entitled EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances. This paper was eventually accepted for publication and appeared in the 20th NISSC proceedings published on October 9, 1997. ("EMERALD 1997"). The purpose of this article was to provide an overview of the project at SRI that had recently obtained DARPA funding and to outline the research we intended to pursue, the ultimate goal of which was to develop a scalable system for detecting suspicious network activity in high-speed distributed computer networks.

6. At the time we prepared EMERALD 1997, SRI was just beginning the EMERALD project. Certainly, the required experimentation needed to adapt the statistical detection concepts from SRI's prior IDES and NIDES programs to the analysis of network traffic had not yet substantially begun. Subsequent to the preparation and submission of the EMERALD 1997 article a great deal of time, effort and research funding was expended in the work related to achieving a workable system for applying

the statistical anomaly detection concepts to the specific environment of network traffic analysis in which EMERALD was designed to be employed.

**BEST MODE: detecting suspicious activity**

7. As of November 9, 1998, when my co-inventor and I filed the patents-in-suit, the focus of what I considered to be our "invention" was two fold; 1) the application of statistical anomaly detection techniques to the problem of detecting suspicious activity in a large network and 2) the building of an analysis hierarchy that would allow distributed analysis and scalability while also allowing a system to recognize distributed activity that might go unnoticed by a "local" detector.

8. In November 1998, I believed that statistical methodologies offered a potentially promising and important complement to existing "signature" techniques for the detection of suspicious network activity. Statistical techniques allow for the detection of previously unknown attacks, something that cannot be effectively achieved by signature-based analysis. This focus is reflected in the first patent we filed, which issued as the '338 patent, the claims of which are specifically directed to statistical profiling techniques. The initial implementation of the statistical detection invention became known as the "eStat" module of the network intrusion detection system.

9. The inventions claimed in the later patents, specifically the '203 and '615 patents, reflect the analysis hierarchy aspect of our invention. The '212 patent, which was filed last in the series, claims the analysis hierarchy with the lowest level "detection" being performed using statistical detection techniques.

10. In November 1998, with regard to the "hierarchy" aspects of our invention, I believed that what was essential to the invention was the confining of the lowest level of the analysis to a subset of the available network traffic data, combined with the analytical hierarchy that further allowed analyzing large amounts of network data in an efficient manner. What was important was the data that the lowest level "monitors" analyzed to determine suspicious activity and generate "alerts" and how those alerts were passed to

higher-level monitors for further analysis. I believed that various types of intrusion detection systems, including those that used statistical or signature-based algorithms, could be used in the hierarchy. I did not consider the specific type of detection technique performed at the lowest level of the hierarchy to be particularly important to the invention and, in fact, intended the hierarchy invention to be somewhat independent of the specific type of detection employed.

11. I do not believe and did not believe in November 1998 that our invention required the use of any particular type of signature detection technique. Signature analysis on its own was not a significant component of our invention. Representative examples of signature detection techniques that could optionally be used in the hierarchical architecture of our inventions were described in the specifications of the patents-in-suit as possible ways to detect suspicious network activity.

12. As of November 1998, signature-based techniques of network intrusion detection were fairly well-known and established in the art of computer security. Numerous different signature-based systems were publicly available, including, for example, Network Flight Recorder and ISS RealSecure. After initial consideration early in the EMERALD project of using such a tool, the decision was made to develop in-house a signature-based detection capability specifically for our network intrusion detection system. This development eventually led to a series of computer software modules we referred to as the "eXpert" modules

13. At the time the first EMERALD-related patent was filed in November, 1998, I did not consider the eXpert modules we were developing to be superior to any of the other publicly available signature-based technologies. In fact, a great deal of effort was made in the 1999 timeframe on the eXpert modules to improve their usefulness. Nor did I consider, as of November 1998, signature-based detection techniques to be inherently superior to statistical techniques for detecting suspicious network activity in general,

although in specific circumstances signature techniques could be more effective at dealing with known types of attacks. I viewed these techniques as complementary.

LINCOLN LABS TESTING

14. On November 9, 1998, the morning after several colleagues and I submitted the results of tests performed at the Lincoln Laboratory of the Massachusetts Institute of Technology ("Lincoln Labs"), I sent an email message to Ulf Lindqvist. [Ex. P to 2d Moore Decl.]

15. In the message, I wrote that "Keith and Al didn't produce meaningful results with estat. I caught all of our attack results with eXpert, but nearly died trying to do it."

16. The Lincoln Labs test results, namely that eXpert (a signature technique) detected more attacks in the 1998 Lincoln Labs testing than eStat (a statistical technique), did not change my belief that statistical detection techniques offered a useful complement to signature detection techniques for the detection of suspicious activity.

17. It was something of a surprise that eStat didn't perform better during the Lincoln Labs test, but I eventually came to understand that the network traffic data used in the 1998 Lincoln Labs tests was skewed towards signature techniques. At that point, eXpert's relatively stronger performance than eStat made sense to me. Within a few months of getting the test results, I explained this aspect of the Lincoln Labs test dataset to my colleagues. Part of this discussion is reflected in an email I sent on July 2, 1999 discussing the shortcomings of the Lincoln Labs test in fairly assessing statistical detection systems REDACTED

18. We did not "abandon" eStat or statistical detection techniques shortly after or as a result of the 1998 Lincoln Labs testing. SRI continued to develop and use eStat until at least early 2000. SRI also later developed other statistical detection techniques that were incorporated into other software modules, such as what became known as "eBayes," that continue to be part of the EMERALD system.

**EMERALD eXpert/estat TCP/UDP/ICMP analysis summary**

19. I wrote the October 16, 1998 draft of the EMERALD eXpert/estat/TCP/UDP/ICMP ANALYSIS SUMMARY (Ex. L to 2d Moore Decl.).

20. This analysis summary was, as I stated in the document, highly preliminary. The hypotheses in the document were untested. The analysis summarized in the document focused on the detection of well-known attacks, which, generally speaking, signature engines are more adept at detecting than statistical algorithms.

21. The number of these attacks detected by the eStat module as opposed to the eXpert module does not provide any indication as to which is "better" for the detection of suspicious network activity; either in general or in a specific environment. I do not believe that, as of the time I prepared this memo, I had reached any firm conclusions on the subject, other than to have recognized that signature-based techniques would likely be better suited to detecting certain types of known attacks. Certainly I did not believe that signature-based techniques would be superior to statistical detection under all circumstances. Nor did I believe signature-based techniques would be more or less appropriate in the context of my inventions which, as explained above, were intended to be independent of detection technique or were specifically directed to statistical techniques rather than use of signatures.

22. The analysis summary memo also indicates that the "etcpgen" module was still under development. Its functional requirements had not yet been completely specified.

**BEST MODE: receiving network packets**

23. As of November 1998, many techniques for receiving network packets or "sniffing" packets off a network, were well-known and publicly available, including Network Flight Recorder and ISS RealSecure.

24. I do not believe now and did not believe in November 1998 that our inventions that became the subject of the patents in this case required the use of any

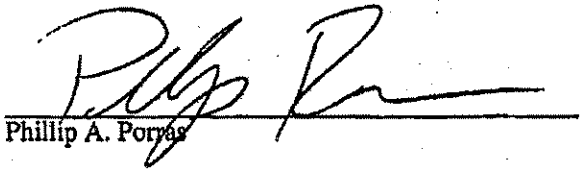
particular techniques for pulling packets off a network. Packet-sniffing on its own was not a significant component of our inventions. As explained above, what was important was the identification of the subset of traffic to be analyzed, which is described in the patents, after the packets had been obtained off the network.

25. Prior to and during November 1998, SRI was exploring and experimenting with several different techniques for receiving network packets, including the use of Network Flight Recorder, a publicly available software product. In the middle of 1998, a decision was made to attempt to develop, in-house, a module or modules that could perform the packet sniffing functions. One of the modules we developed for this became known as "etcpgen".

26. As of November 9, 1998, it was unclear which, if any, of the various approaches to obtaining and processing network packets we were considering would be preferable for use in the actual implementation of our live network IDS implementation.

27. As of November 1998, these modules, including etcpgen, were still under development and frequently being rewritten. As noted above, the October 16, 1998 memo I wrote indicated that, as of that time, we were still working on defining the functional specifications for the module.

I declare under penalty of perjury under that the foregoing is true and correct. Executed this 30th day of June 2006, in Menlo Park, California.



Phillip A. Porras

50355817.doc

# EXHIBIT A

REDACTED

**CERTIFICATE OF SERVICE**

I hereby certify that on July 10, 2006, I electronically filed the **REDACTED – DECLARATION OF PHILLIP A. PORRAS IN SUPPORT OF SRI INTERNATIONAL, INC.'S RESPONSE TO DEFENDANTS' JOINT MOTION FOR SUMMARY JUDGMENT THAT SRI INTERNATIONAL, INC.'S PATENTS ARE INVALID FOR FAILURE TO DISCLOSE BEST MODE AND DEFENDANTS' JOINT MOTION FOR SUMMARY JUDGMENT OF INVALIDITY PURSUANT TO 35 U.S.C. §§ 102 AND 103** with the Clerk of Court the attached document using CM/ECF which will send electronic notification of such filing(s) to the following Delaware counsel.

Richard L. Horwitz
Potter Anderson & Corroon LLP
Hercules Plaza
1313 North Market Street, 6th Floor
P.O. Box 951
Wilmington, DE 19899

Attorneys for Defendant-Counterclaimant Internet Security Systems, Inc., a Delaware corporation, and Internet Security Systems, Inc., a Georgia corporation

Richard K. Herrmann
Morris James Hitchens & Williams
PNC Bank Center
222 Delaware Avenue, 10th Floor
P.O. Box 2306
Wilmington, DE 19899-2306

Attorneys for Defendant-Counterclaimant Symantec Corporation

/s/ *John F. Horvath*
John F. Horvath

80034097.doc